UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/624,403	07/21/2003	Kevin E. Fu	200311171-1	6808

22879 7590 06/06/2008

HEWLETT PACKARD COMPANY
P O BOX 272400, 3404 E. HARMONY ROAD
INTELLECTUAL PROPERTY ADMINISTRATION
FORT COLLINS, CO 80527-2400

EXAMINER	
CHEN, SHIN HON	
ART UNIT	**PAPER NUMBER**
2131	

NOTIFICATION DATE	DELIVERY MODE
06/06/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

JERRY.SHORMA@HP.COM
mkraft@hp.com
ipa.mail@hp.com

Office Action Summary	Application No.	Applicant(s)	
	10/624,403	FU ET AL.	
	Examiner	Art Unit	
	SHIN-HON CHEN	2131	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *06 July 2007*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-21* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-21* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *21 July 2003* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-21 have been examined.

Claim Rejections - 35 USC § 102

2. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (a) the invention was known or used by others in this country, or patented or described in a printed publication in this or a foreign country, before the invention thereof by the applicant for a patent.

3. Claims 1, 2, 4-6, and 8-13 and 15-21 are rejected under 35 U.S.C. 102(a) as being anticipated by Hardy et al. U.S. Pub. No. 20020152392 (hereinafter Hardy).

4. As per claim 1, Hardy discloses a method of windowed backward key generation, comprising: a) providing information to a user that allows determining a limited number of previous keys in a series of keys from a later key in the series and wherein said information is derived from at least one of said limited number of previous key in said series (Hardy: [0007]: provide keys in sequential order backward or forward; [0021]: provide UPDATE SPLIT/information to user for subsequent or previous version and the UPDATE SPLIT is derived from the previous key and the later key); b) generating a key in the series, based at least in part on said information provided to said user (Hardy: [0015] and [0021]: split is used to generate new key); c) providing said key in the series to the user (Hardy: [0015]: initial key A is provided to user); and d) said user determining at least one key in the limited number of previous keys in the series by applying said information to said key in the series provided to the user

(Hardy: [0021]: generate different preceding or subsequent keys sequentially or non-sequentially based on the initial key and updated split).

5. As per claim 2, Hardy discloses the method of claim 1. Hardy further discloses providing a key rotation element that is forward rotatable by said user but is not backward rotatable (Hardy: [0021]: key is forward rotatable when the key split is intended for forward rotation).

6. As per claim 4, Hardy discloses the method of claim 2. Hardy further discloses the method comprising: e1) generating a new key rotation element (Hardy: [0021]: generate updated split); e2) generating a new key based, in part, on said new key rotation element (Hardy: [0021]: generate new key); and e3) distributing said new key to non-revoked users (Hardy: [0021]: user can now use the new key).

7. As per claim 5, Hardy discloses the method of claim 1. Hardy further discloses wherein said a) further comprises providing a secret share and a key rotation catalyst to said user (Hardy: [0021]: the token and split), wherein said secret share and said key rotation catalyst allow said user to generate a next key in the series provided sufficient public information is available (Hardy: [0021]: updated split can be public).

8. As per claim 6, Hardy discloses the method of claim 5. Hardy further discloses further comprising: e) publishing at least one public share, wherein the next key in the series is

determinable based on the key rotation catalyst, the secret share, and the at least one public share (Hardy: [0021]: the updated split, the token, and the initial key split).

9. As per claim 8-13 and 15-21, claims 8-13 and 15-21 encompass the same scope as claims 1, 2, and 4-6. Therefore, claims 8-13 and 15-21 are rejected based on the same reasons set forth above in rejecting claims 1, 2, and 4-6.

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 3, 7 and 14 are rejected under 35 U.S.C. 103(a) as being unpatentable over Hardy.

12. As per claim 3, Hardy discloses the method of claim 1. Hardy further discloses that the operation involved in the key generation is logical addition (Hardy: [0021]: exclusive OR). Hardy does not explicitly disclose wherein said a) comprises providing to the user a key rotation exponent that is used to determine a previous key in the series from a later key in the series by exponentiating said later key by said key rotation exponent. However, it would have been obvious to one having ordinary skill in the art to utilize exponentiation in place of the logical addition in computing updated key because mathematical formulas can be interchangeably used

to compute cryptographic keys when the underlying concept permits the operation to be successful.

13. As per claim 7 and 14, Hardy discloses the method of claims 5 and 12. Hardy does not explicitly disclose revoking a user by publishing a version of the revoked user's secret share. However, it would have been obvious to one having ordinary skill in the art to publish the private share of the revoked user because the published private share of revoked user undergoing logical addition with private share of the revoked user would generate useless data.

Response to Arguments

14. Applicant's arguments filed 7/6/07 have been fully considered but they are not persuasive.

Regarding applicant's remarks, applicant argues that the Key B is a new decryption key which is not related or derived from a series of previous keys in a series and is therefore of no use in determining any previous keys in a series of keys. However, the limitations argued by the applicant cannot be found within the claims (the claim is recites that "**the information**" is derived from at least one of said limited number of previous keys in said series, not "**Key B**"). Therefore, the examiner is not required to address that limitation.

On the other hand, claim 1 disclose "said key" in the claim without explicitly referring to one of previously mentioned keys. Therefore, the examiner has examined the application with broadest reasonable interpretation.

Conclusion

15. The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

Candelore U.S. Pat. No. 6363149 discloses method for accessing stored digital programs by deriving past keys.

16. Applicant's amendment necessitated the new ground(s) of rejection presented in this Office action. Accordingly, **THIS ACTION IS MADE FINAL**. See MPEP § 706.07(a). Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Shin-Hon Chen whose telephone number is (571) 272-3789. The examiner can normally be reached on Monday through Friday 8:30am to 5:30pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free)? If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Ayaz R. Sheikh/
Supervisory Patent Examiner, Art Unit 2131

Shin-Hon Chen
Examiner
Art Unit 2131

SC